

RSAConference2019 **Asia Pacific & Japan**

Singapore | 16–18 July | Marina Bay Sands



BETTER.

SESSION ID: **SDS-R04**

Distributed forensic collection and analysis

Dr Michael Cohen

Digital Paleontologist
Velocidex Enterprises

Nick Klein

Director, Velocidex Enterprises
Director, Klein & Co. Computer Forensics
SANS DFIR Certified Instructor

Who are we?

Dr Michael Cohen

- Experienced digital forensic software developer
- Developer of foundation forensic tools including Volatility and Rekall
- Former lead developer of Grr Rapid Response at Google Inc.



Nick Klein

- Director of Klein & Co. digital forensic and cyber response team
- SANS DFIR Certified Instructor



What's the challenge?

Deep visibility of endpoints is a game changer for digital forensic investigations, threat hunting and cyber breach response.

Many endpoint monitoring products now exist, but there are few powerful tools to **truly interrogate and collect historic evidence** from across a network.

For example, an EDR tool may show network connections, but can it also interrogate the Internet history of all users?

We're building Velociraptor to address these limitations.

Why Velociraptor?

Velociraptor is a unique DFIR tool, giving *you* power and flexibility through the Velociraptor Query Language (VQL)

VQL is used for everything:

- Collecting information from endpoints
- Controlling monitoring and response
- Controlling and managing the server



Easy server setup

```
C:\Program Files\Velociraptor>
?
Welcome to the Velociraptor
-----
I will be creating a new
begin by identifying what

Self Signed SSL
Generating keys please wa
? Enter the frontend port
? What is the public DNS
? Path to the datastore d
? Path to the logs direct
? Where should i write th
? Where should i write th
? GUI Username or email a
? GUI Username or email a

C:\Program Files\Velociraptor>
```



Deploying clients

Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.107]

(c) 2018

C:\WINDOWS

C:\Program

C:\Program

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name

Velociraptor

Velociraptor

Windows

Windows

Windows

Windows

Windows

wininit

winlog

Fewer

desktop

DESKTOP-6CBJ8MJ connected

Interrogate

VFS

Collected

Overview

VQL Drilldown

DESKTOP-6CBJ8MJ

Client ID	C.e57080a99511ee58
Agent Version	2019-06-30T11:35:47+10:00
Agent Name	velociraptor
Last Seen At	2019-06-30 09:47:34 UTC
Last Seen IP	[::1]:49910

Operating System	windows
Hostname	DESKTOP-6CBJ8MJ
Release	Microsoft Windows 10 Enterprise10.0.17763 Build 17763
Architecture	amd64

2019-06-30 09:55:26 UTC

Use Velociraptor artifacts to automate everything

We can collect information about *many* things in DFIR cases:

- Registry keys, files, WMI queries, Sqlite databases ...

But we often need to answer specific questions:

- What program did the attacker run?
- What files were downloaded?
- What DNS lookups occurred?
- Did a particular file exist on an endpoint?

Use expert knowledge to find the evidence

A key objective of Velociraptor is encapsulating DFIR knowledge into the tool:

- We have high level questions to answer
- We know where to look for evidence of user / system activities

We build artifacts to collect and analyze the evidence in order to answer our investigative questions.

Single endpoint collection

desktop

DESKTOP-6CBJ8MJ connected

0 mic

ntuser

Windows.Registry.NTUser

Windows.Registry.NTUser.Upload

Windows.Registry.NTUser.Upload

Type: client

This artifact collects all the user's NTUser.dat registry hives.

When a user logs into a windows machine the system creates their own "profile" which consists of a registry hive mapped into the HKEY_USERS hive. This hive file is locked as long as the user is logged in.

This artifact bypasses the locking mechanism by extracting the registry hives using raw NTFS parsing. We then just upload all hives to the server.

Source

```
1 LET users = SELECT Name, Directory as HomeDir
2   FROM Artifact.Windows.Sys.Users()
3   WHERE Directory
4 SELECT upload(file="\\\\.\\\\" + HomeDir + "\\ntuser.dat",
5   accessor="ntfs") as Upload
6 FROM users
7
8
```

Hunting is the collection of artifacts across the network

Any artifact that can be collected on a single computer, can be hunted across the network

A hunt can cover a group of clients, or the whole network

A hunt will continue running until it expires, or is stopped

As new machines appear, they automatically join in the hunt

Network-wide hunts

desktop

+

▶

■

New Hunt - Select Artifact

Step 1 out of 5

ntus

Windows.Registry.NTUser

Windows.Registry.NTUser.Upload

Selected Artifacts:

Windows.Registry.NTUser.Upload

Clear

Ons/Sec

desktop

+

▶

■

DESKTOP-6CBJ8MJ

connected

0

mic

Status	Hunt ID	Description	Create Time	Start Time	Expires	Client Limit	Clients Scheduled	Creator
⌵	H.b7c9e52e		2019-06-30 22:41:47 UTC	2019-06-30 22:41:51 UTC	2019-07-07 22:41:47 UTC	Unlimited	2	mic

Overview

Results

Clients

Report

Windows.Registry.NTUser.Upload

Show 10 entries

Search:

Upload	FlowId	ClientId	Fqdn
Path : \\IC:\Users\test\ntuser.dat Size : 1572864 md5 : 589cf495f69947a760babe780b85cd80 sha256 : ad3de1e57954405ae93a133d6f51049b440e5a30f42a485effd0a5271f59a306	F.BKCJLCE2V4UP2	C.e57080a99511ee58	DESKTOP-6CBJ8MJ
Path : \\IC:\Users\test\ntuser.dat Size : 1572864 md5 : 589cf495f69947a760babe780b85cd80 sha256 : ad3de1e57954405ae93a133d6f51049b440e5a30f42a485effd0a5271f59a306	F.BKCJLCIQBUDQ4	C.e57080a99511ee58	DESKTOP-6CBJ8MJ

Activate Windows

Go to Settings to activate Windows.

2019-06-30 22:43:35 UTC



Scenario: Finding files across endpoints

Searching for files is a fundamental capability.

Velociraptor provides a powerful **File Finder** artifact for this.

- Use wildcards to 'glob' over directories
- Use Yara to search the contents of files for keywords
- Filter by modified or created dates
- Upload matching files to the server, for further analysis.

The **Windows.Search.FileFinder** is a great start for many custom artifacts - just copy/paste and pre-populate with the right defaults.

Scenario: Finding files across endpoints

New Artifact Collection - Select Artifacts to collect
Step 1 out of 2

Selected Artifacts:

- Windows.Search.FileFinder

Clear Remove

SearchFilesGlob ☐

Keywords ☐

Use_Raw_NTFS ☒

Upload_File ☐

Calculate_Hash ☐

MoreRecentThan

ModifiedBefore

Calendar: July 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	30	01	02	03	04	05
28	07	08	09	10	11	12
29	14	15	16	17	18	19
30	21	22	23	24	25	26
31	28	29	30	31	01	02
32	04	05	06	07	08	09

Today Clear Close

2019-07-02

Select Artifacts to collect

Next

Scenario: Hunt for evidence of program execution

Program Execution

UserAssist

Description

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

Location

NTUSER.DAT\HIVE:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
(GUID)\Count

Interpretation

All values are ROT-13 Encoded

- GUID for XP
 - 75048700 Active Desktop
- GUID for Win7/8/10
 - CEBFF5CD Executable File Execution
 - F4E57C4B Shortcut File Execution

Windows 10 Timeline

Description

Win10 records recently used applications and files in a "timeline" accessible via the "WIN+TAB" key. The data is recorded in a SQLite database.

Location

C:\Users\profile\AppData\Local\ConnectedDevices
PlatformL_profile\ActivitiesCache.db

Interpretation

- Application execution
- Focus count per application

RecentApps

Description

GUI Program execution launched on the Win10 system is tracked in the RecentApps key

Location

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps

Interpretation

Each GUID key points to a recent application.
AppID = Name of Application
LastAccessTime = Last execution time in UTC
LaunchCount = Number of times executed

Shimcache

Description

- Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.
- Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

Location

XP:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility
Win7/8/10:
SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache

Interpretation

Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.

- Windows XP contains at most 96 entries
 - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
 - LastUpdateTime does not exist on Win7 systems

Jump Lists

Description

- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.

Location

Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- First time of execution of application.
 - Creation Time = First time item added to the AppID file.
 - Last time of execution of application w/ file open.
 - Modification Time = Last time item added to the AppID file.
- List of Jump List IDs ->
http://www.forensicswiki.org/wiki/List_of_Jump_List_Ids

Amcache.hve

Description

ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file Amcache.hve to store data during process creation

Location

Win7/8/10:
C:\Windows\AppCompat\Programs\Amcache.hve

Interpretation

- Amcache.hve - Keys = Amcache.hve\Root\File\Volume GUID\#####
- Entry for every executable run, full path information, File's \$StandardInfo Last Modification Time, and Disk volume the executable was run from
- First Run Time = Last Modification Time of Key
- SHA1 hash of executable also contained in the key

System Resource Usage Monitor (SRUM)

Description

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Location

SOFTWARE\Microsoft\Windows\NT\CurrentVersion\SRUM\Extensions\{d10ca2fe-6fcd-416d-948e-b2c9926fa89} = Application Resource Usage Provider C:\Windows\System32\SRUM

Interpretation

Use tool such as `srum_dump.exe` to cross correlate the data between the registry keys and the SRUM ESE Database.

BAM/DAM

Description

Windows Background Activity Moderator (BAM)

Location

Win10:
SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
SYSTEM\CurrentControlSet\Services\diam\UserSettings\{SID}

Investigative Notes

Provides full path of the executable file that was run on the system and last execution date/time

Last-Visited MRU

Description

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.
Example: Notepad.exe was last run using the C:\%USERPROFILE%\Desktop folder

Location

XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Interpretation

Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

Prefetch

Description

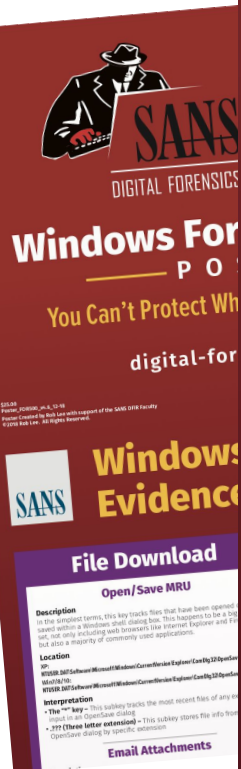
- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8
- (exename)-(hash).pf

Location

WinXP/7/8/10:
C:\Windows\Prefetch

Interpretation

- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- Date/Time file by that name and path was first executed
 - Creation Date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
 - Embedded last execution time of .pf file
 - Last modification date of .pf file (-10 seconds)
 - Win8-10 will contain last 8 times of execution



	Windows.Persistence.PersistentWMIEvents				
	Windows.Persistence.PowershellRegistry				
✓	F.BKCA7I24JO2NK	Windows.Analysis.EvidenceOfExecution	2019-06-30 11:58:00 UTC	2019-06-30 11:58:05 UTC	mic
✓	F.BKCA5KPQ7P26E	Windows.Applications.Chrome.History	2019-06-30 11:53:55 UTC	2019-06-30 11:53:56 UTC	mic
✓	F.BKC8TJ3DDSN2	Windows.Registry.NTUser.Upload	2019-06-30 10:28:28 UTC	2019-06-30 10:28:30 UTC	mic
	F.BKC9DSK7AQUM	VESDownloadFile	2019-06-30 00:54:59 UTC	2019-06-30 00:55:00 UTC	mic
C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe			1561289157	2019-06-23T11:25:57Z	
C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe			1561289157	2019-06-23T11:25:57Z	
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe			1554134407	2019-04-01T16:00:07Z	
Showing 1 to 10 of 203 entries			Previous	1	2 3 4 5 ... 21 Next

Scenario: Hunt for an APT group using threat intel

The screenshot shows the MITRE ATT&CK website. The browser address bar displays `attack.mitre.org`. The page title is "APT30". The sidebar on the left lists various groups, with "APT30" highlighted. The main content area provides an overview of the group and a table of associated software.

MITRE ATT&CK

Matrices Tactics Techniques Groups Software
Resources Blog Contribute

Search site

Home > Groups > APT30

APT30

APT30 is a threat group suspected to be associated with the Chinese government. [1] While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches. [2]

ID: G0013
Version: 1.0

Software

ID	Name	References	Techniques
S0031	BACKSPACE	[1]	Command-Line Interface, Connection Proxy, Data Obfuscation, Disabling Security Tools, Exfiltration Over Command and Control Channel, File and Directory Discovery, Modify Registry, Multi-Stage Channels, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery
S0036	FLASHFLOOD	[1]	Data Encrypted, Data from Local System, Data from Removable Media, Data Staged, File and Directory Discovery, Registry Run Keys / Startup Folder
S0034	NETEAGLE	[1]	Command-Line Interface, Custom Command and Control Protocol, Exfiltration Over Command and Control Channel, File and Directory Discovery, Modify Registry, Multi-Stage Channels, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery

GROUPS

- Overview
- admin@338
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30**
- APT32
- APT33
- APT37
- APT38

APT32

Also known as: OceanLotus G

Suspected attribution: Vietna

Target sectors: Foreign comp
manufacturing, consumer pr

Overview: Recent activity ta
suggests that APT32 poses
manufacturing or preparing
motivation for this activity
the competitive advantage

Associated malware: SOU
KOMPROGO

Attack vectors: APT32 ac
social engineering metho
Upon execution, the initia

Scenario: Hunt for an APT group using threat intel

The screenshot displays the Velociraptor web interface. On the left, a sidebar shows a list of artifacts, including 'Custom.IOC.File.Hashmatch'. A modal window titled 'Add/Modify an artifact' is open, showing the configuration for 'Custom.IOC.File.Hashmatch'.

Add/Modify an artifact configuration:

```

1 name: Custom.IOC.File.Hashmatch
2 description: |
3   This looks for specific files that have been associated with indicators of compromise. These files should be placed in the IOCFiles parameter.
4
5 parameters:
6   - name: IOCFiles
7     default: |
8       ["**/*20/*.pdf", "**/*20/*.xlsx", "**/*20/*.xls", "**/*20/*.doc", "**/*20/*.docx"]
9   - name: Hashlist
10    default: |
11      ["0062B64CB29B1749E40E670B44B2668B", "009DE217B53E6535F5EE196876B4A3F5", "FEB4B512EE174A0A2459428", "FF51E0A2459428", "FF96C36977D620"]
12
13 sources:
14   - queries:
15     - |
16       LET FilesToHash = SELECT FullPath, Created, Modified, Accessed, size
17         FROM glob(globs=parse_json_array(data=IOCFiles))
18         WHERE size < 104857600
19     - |
20       SELECT FullPath, Created, Modified, Accessed, size,
21         hash(path=FullPath).md5 as MD5 from FilesToHash
22       where MD5 in Hashlist
  
```

On the right, the 'Custom.IOC.File.Hashmatch' artifact details are shown. It includes a description, parameters, and a source query.

Custom.IOC.File.Hashmatch Details:

- Type: client
- Description: This looks for specific files that have been associated with indicators of compromise. These files should be placed in the IOCFiles parameter.
- Parameters:

Name	Default
IOCFiles	["**/*20/*.pdf", "**/*20/*.xlsx", "**/*20/*.xls", "**/*20/*.doc", "**/*20/*.docx"]
Hashlist	["0062B64CB29B1749E40E670B44B2668B", "009DE217B53E6535F5EE196876B4A3F5", "FEB4B512EE174A0A2459428", "FF51E0A2459428", "FF96C36977D620"]
- Source:


```

1 LET FilesToHash = SELECT FullPath,
2   timestamp(epoch=Ctime.sec) as Created,
3   timestamp(epoch=Mtime.sec) as Modified,
4   timestamp(epoch=Atime.sec) as Accessed,
5   size from glob(globs=parse_json_array(data=IOCFiles))
6   WHERE size < 104857600
7 SELECT FullPath, Created, Modified, Accessed, size,
8   hash(path=FullPath).md5 as MD5 from FilesToHash
9 WHERE MD5 in Hashlist
10
  
```


Scenario: Hunt down “shadow IT”

Dropbox is one common “shadow IT” threat.

It can be accessed through a web browser or an installed program.

Questions we may want to answer from our endpoints:

- Which users have Dropbox accounts?
- Which users have Dropbox installed locally?
- When did they access Dropbox through their web browsers?
- What confidential documents are shared through Dropbox?



State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
✓	F.BKE9AQUGNA20S	Windows.Applications.Chrome.History Windows.Applications.Chrome.Extensions Windows.Applications.Chrome.Cookies	2019-07-03 11:45:47 UTC	2019-07-03 11:45:56 UTC	mic
✓	F.BKE987AQPQP7S	Windows.Applications.Chrome.Extensions	2019-07-03 11:40:13 UTC	2019-07-03 11:40:16 UTC	mic

Artifact CollectionUploaded FilesRequestsResultsLogReports

Windows.Applications.Chrome.History

Windows.Applications.Chrome.History

Show 10 entries

Search: drop

User	FullPath	Mtime	visited_url
test	\\C:\\Users\\test\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2019-07-03T11:44:35Z	https://chrome.google.com/webstore/search/dropbox
test	\\C:\\Users\\test\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2019-07-03T11:44:35Z	https://www.google.com/search?q=dropbox&rlz=1C1CHBF_enAU843AU843&oq=dropbox&aqs=chrome..69i57j0l5.1871j0j7&sourceid=chrome&ie=L8
test	\\C:\\Users\\test\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2019-07-03T11:44:35Z	https://www.dropbox.com/
test	\\C:\\Users\\test\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\History	2019-07-03T11:44:35Z	https://www.dropbox.com/individual



State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
✓	F.BKE9AQUGNA20S	Windows.Applications.Chrome.History Windows.Applications.Chrome.Extensions Windows.Applications.Chrome.Cookies	2019-07-03 11:45:47 UTC	2019-07-03 11:45:56 UTC	mic
✓	F.BKE987AQPQP7S	Windows.Applications.Chrome.Extensions	2019-07-03 11:40:13 UTC	2019-07-03 11:40:16 UTC	mic

Artifact Collection

Uploaded Files

Requests

Results

Log

Reports

Windows.Applications.Chrome.Cookies

Windows.Applications.Chrome.Cookies

Show 10 entries

Search: dropbox

Created	LastAccess	Expires	host_key	name	path	value	EncryptedValue
2019-07-03T11:41:36Z	2019-07-03T11:44:48Z	2024-07-01T11:41:36Z	www.dropbox.com	gvc	/		AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rIOqqOQAAAAACAAAA
2019-07-03T11:41:36Z	2019-07-03T11:44:41Z	2024-07-01T11:41:36Z	.dropbox.com	locale	/		AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rIOqqOQAAAAACAAAA
2019-07-03T11:41:37Z	2019-07-03T11:45:03Z	2020-07-02T11:41:38Z	.dropboxstatic.com	__cfduid	/		AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rIOqqOQAAAAACAAAA
2019-07-03T11:41:42Z	2019-07-03T11:44:59Z	2019-10-01T11:41:42Z	.dropbox.com	_gcl_au	/		AQAAANCMnd8BFdERjHoAwE/CI+sBAAAA3LhKs5AJj0+0gz+rIOqqOQAAAAACAAAA

2019-07-02 22:49:42 UTC

Scenario: Use of Microsoft SysInternal tools

SysInternal tools are powerful system administration tools which are also used by attackers “living off the land”.

Did any SysInternal tools ever run on your endpoint?

For non-administrator accounts, this is very suspicious.

Hint: Sysinternals tools require the user accepting a EULA, which leaves an interesting forensic artifact - a Registry key showing the user accepted the EULA.

We have an artifact for that too!



Search Box



DESKTOP-6CBJ8MJ

connected

0

mic



State	FlowId	Artifacts Collected	Creation Time	Last Active	Creator
	F.BKE9L7U4IOJN6	Windows.Registry.Sysinternals.Eulacheck	2019-07-03 12:07:59 UTC	2019-07-03 12:07:59 UTC	mic

Artifact Collection

Uploaded Files

Requests

Results

Log

Reports

Windows.Registry.Sysinternals.Eulacheck

Windows.Registry.Sysinternals.Eulacheck

Show 10 entries

Search:

ProgramName	Key	TimeAccepted	User	EulaAccepted
PsExec	HKEY_USERS\S-1-5-21-1959620319-2477567439-3049586023-1001\Software\Sysinternals\PsExec	2019-06-28T13:53:29Z	test	1
PsList	HKEY_USERS\S-1-5-21-1959620319-2477567439-3049586023-1001\Software\Sysinternals\PsList	2019-06-28T13:53:29Z	test	1

Showing 1 to 2 of 2 entries

Previous 1 Next

Scenario: Monitor all DNS lookups

DNS lookups are an *excellent* network signal.

They can reveal C2 activity and help scope the extent of compromise across a network by showing all clients attempting to connect to known-bad domains.

We can store all DNS lookups from clients, then search this data when threat intel reveals C2 and other suspicious DNS names.



Search Box



DESKTOP-6CBJ8MJ

connected

0

mic



Windows.Events.DNSQueries ▾

2019-07-02



DNS Questions for DESKTOP-6CBJ8MJ

The 1000 most common DNS Queries on this day are listed in the below table. Typically we are looking for two interesting anomalies:

1. Sorting by count for the most frequently called domains. If you do not recognize these it may be possible that a malware is frequently calling out to its C&C.
2. Examining some of the least commonly used DNS names might indicate DNS exfiltration.

Show 10 ▾ entries

Search:

Total	Name
2	assets.msn.com.
2	ocsp.pki.goog.
2	img-s-msn-com.akamaized.net.
2	about.google.
2	secure-au.imrworldwide.com.
2	www.google.com.
1	googleads.g.doubleclick.net.
1	adservice.google.com.
1	www.google.com.au.
1	sam.msn.com.

Showing 1 to 10 of 30 entries

Previous

1

2

3

Next

Velociraptor can hunt for whatever information exists across your endpoints.

So, what do *you* want to find?

Watch this space

Velociraptor is **free and open source** - download and use it today

Ongoing professional development, plus contributions from the DFIR community

Velociraptor is commercially supported through the availability of training and professional services

Development roadmap

More artefacts – based on investigation and other scenarios

More evidence parsers – for more complete forensic analysis

More monitoring functionality – for real-time event detection

Kernel module – for tighter monitoring integration

Wider OS support – more artefacts for OSX and Linux

User interface – more functionality and workflow.

Start hunting today!

Download Velociraptor: github.com/Velocidex/velociraptor

Review the **Quick Start** documentation

Setup a server and deploy some test agents

Start by hunting for some pre-built artefacts

Then customise some hunts to your own requirements

Contribute back with your feedback and ideas

RSAConference2019 **Asia Pacific & Japan**

Thank you.

<https://github.com/Velocidex/velociraptor>